02_資安事件及異常紀錄 - 非法入侵 #683

TPHQ6WKS324

2024-02-19 10:16 - Joy Liao

狀態:	Closed-關閉	**開始日期:**	2024-02-19
優先權:	Normal	**完成日期:**	2024-02-29
被分派者:	益利 周	**完成百分比:**	100%
分類:		**預估工時:**	0:00 小時
版本:			

概述

Description
A suspicious process injected into another process in an unusual way. Investigate the process trees for the injector and injectee.

Command line
"C:\WINDOWS\system32\rundll32.exe"
D:\Users\ProgramData\Lenovo\Vantage\Addins\LenovoBatteryGaugeAddin\1.0.3.12\x64\LenovoBatteryGaugePackage.dll
UnloadBatteryGaugeFromExplorer

歷史

#1 - 2024-02-26 17:31 - 益利 周

- 狀態 從 New-新增 變更為 In process-進行中

- 完成百分比 從 0 變更為 100

葉虹妤 PC
已移除此電源管理程式.

#2 - 2024-03-21 16:23 - 益利 周

- 狀態 從 In process-進行中 變更為 Resolved-解決

#3 - 2024-04-02 10:02 - Joy Liao

- 狀態 從 Resolved-解決 變更為 Closed-關閉